

## ⑪ 公開特許公報 (A) 平2-173869

⑤Int.Cl.  
G 06 F 15/21  
G 06 K 17/00識別記号 340 B  
V庁内整理番号 7165-5B  
6711-5B

⑪公開 平成2年(1990)7月5日

審査請求 未請求 請求項の数 3 (全5頁)

⑫発明の名称 ICカードを用いた個人認証システム

⑬特願 昭63-329888

⑭出願 昭63(1988)12月27日

⑫発明者	早崎 政美	東京都台東区台東1丁目5番1号	凸版印刷株式会社内
⑬発明者	松村 秀一	東京都台東区台東1丁目5番1号	凸版印刷株式会社内
⑭出願人	今泉 昭一	東京都台東区台東1丁目5番1号	凸版印刷株式会社内
⑮代理人	弁理士 鈴江 武彦	東京都台東区台東1丁目5番1号	外3名

## 明細書

## 1. 発明の名称

ICカードを用いた個人認証システム

## 2. 特許請求の範囲

(1) マイクロコンピュータ、メモリを含む電子回路を搭載してなり、個人認証を必要とする業務における使用者を特定できる情報が電気信号として記憶された個人認証用のICカードと、

前記ICカードに対して特定情報の読み出しを行なう個人認証情報読み出手段と、

を備えて成ることを特徴とするICカードを用いた個人認証システム。

(2) 前記特定情報としては、使用者の暗証番号情報、写真的画像情報、指紋情報、サイン情報のうち、少なくとも写真的画像情報を含むようにしたことを特徴とする請求項(1)項記載のICカードを用いた個人認証システム。

(3) 前記個人認証情報読み出手段としては、暗証番号情報を入力する入力手段と、指紋情報を入力する指紋照合手段と、前記ICカードに記憶さ

れた暗証番号情報、指紋情報、写真的画像情報およびサイン情報を読み出す読み出手段と、前記情報の読み出し処理を制御する機能、読み出した暗証番号情報ならびに指紋情報と入力情報との照合処理を行なう機能、読み出した写真的画像情報とサイン情報ならびに照合結果の表示処理を制御する機能を有するホストコンピュータと、前記ホストコンピュータによる処理内容を表示する表示手段とから成ることを特徴とする請求項(1)項記載のICカードを用いた個人認証システム。

## 3. 発明の詳細な説明

## (産業上の利用分野)

本発明は個人認証を必要とする業務における正当な使用者の使用実態を特定して不正行為を確実に防止し得るようにしたICカードを用いた個人認証システムに関するものである。

## (従来の技術)

従来から、個人認証を必要とする業務等ではその業務における使用者を特定できる情報を磁気カードに記憶させておき、この磁気カードを用い

て特定の使用者を認証する方法が多く採用されてきている。

(発明が解決しようとする課題)

しかしながら最近では、この種のカードを不正な手段で入手して、不正使用するカード犯罪が増えている。そこで、このように不正な手段で入手した個人認証用のカードの不正使用を防止するためには、使用者を特定できる情報、すなわち使用者の暗証番号情報、写真の画像情報、指紋情報、サイン情報等をカードに記述させておくことが考えられるが、従来の磁気カードでは記述容量が少ないため、この種の情報を記述させることができ困難であり、結果として上述のような不正行為を防止できていないのが実状である。

本発明は上述のような問題を解決するために成されたもので、個人認証を必要とする業務における正当な使用者の使用事実を特定して不正行為を確実に防止することが可能なICカードを用いた個人認証システムを提供することを目的とする。

(課題を解決するための手段)

近年、コンピュータおよびコンピュータを利用した電子機器の外部記憶装置として、カード状の部材にマイクロコンピュータやRAM、ROM等のメモリを搭載したいわゆるICカードが、情報記述容量が非常に大きいこと、および高セキュリティ性を有することから開発されてきている。このICカードは、端子を介して外部の端末装置との間で必要な情報の交換および処理が行なわれるようになっている。本発明では、この種のICカードに、使用者の暗証番号情報、写真の画像情報、指紋情報、サイン情報等、その業務における使用者を特定できる情報を予め書込んでおき、このICカードの使用時に、当該ICカードに記述されている情報を読み出して入力情報との照合を行ない、特定の使用者を認証しようとするものである。

以下、上記のような考え方に基づく本発明の一実施例について、図面を参照して詳細に説明する。第1図は、本発明によるICカードを用いた個人認証システムの構成例を示すブロック図であ

上記の目的を達成するために本発明では、マイクロコンピュータ、メモリを含む電子回路を搭載してなり、個人認証を必要とする業務における使用者を特定できる情報(使用者の暗証番号情報、写真の画像情報、指紋情報、サイン情報等)が電気信号として記述された個人認証用のICカードと、ICカードに対して特定情報の読み出しを行なう個人認証情報読み出手段とを備えて構成している。

(作用)

従って、本発明のICカードを用いた個人認証システムでは、使用者の暗証番号情報、写真の画像情報、指紋情報、サイン情報等、その業務における使用者を特定できる情報を記述容量の大きいICカードに予め書込んでおき、このICカードの使用時に、当該ICカードに記述されている情報を読み出して入力情報との照合を行ない、特定の使用者を認証できることにより、正当な使用者以外の者によるカードの不正使用を確実に防止することが可能となる。

(実施例)

る。本実施例の個人認証システムは第1図に示すように、個人認証用のICカード1と、個人認証情報読み出手段2とから構成している。ICカード1は、マイクロコンピュータ(MPU)11と、EEPROM等からなるメモリ12とを、アドレスバス13およびデータバス14により接続して成っている。また、個人認証情報読み出手段2は、キーボード等よりなる入力手段21と、指紋照合手段22と、読み出手段23と、ホストコンピュータ24と、CRT等よりなる表示手段25とから成っている。

ここで、ICカード1は、個人認証を必要とする業務における使用者を特定できる情報(以下、特定情報と称する)、すなわち使用者の暗証番号情報、写真の画像情報、指紋情報、サイン情報等を、予め電気信号としてそれぞれのエリアに第2図に示す如く記述しているものである。また、入力手段21は、使用者の暗証番号情報を入力するためのものである。指紋照合手段22は、使用者の指紋情報を入力するためのものである。読み出

段23は、上記各情報をICカード1から読み出すためのものである。ホストコンピュータ24は、情報の読み出し処理を制御する機能、読み出した暗証番号情報ならびに指紋情報と入力情報との照合処理を行なう機能、読み出した写真の画像情報とサイン情報ならびに照合結果の表示処理を制御する機能を有するものである。表示手段25は、ホストコンピュータ24による処理内容を表示するためのものである。

次に、以上のように構成した個人認証システムの具体的な動作について、第3図に基づいて説明する。なお、第3図はICカード1からの情報の読み出しを示すフロー図である。

まず、ICカード1が読み出手段23に挿入されたか否かが判定される(ステップS1)。その結果、ICカード1が挿入された場合には、ICカード1から暗証番号情報が読み出手段23により読み出される(ステップS2)。次に、カード使用者により暗証番号情報が入力手段21から入力されると(ステップS3)、この入力された暗証番号

情報と読み出された暗証番号情報とが照合される(ステップS4)。その結果、暗証番号情報が一致していない場合には、そのICカード1の正当な使用者ではない旨が表示手段25に表示される(ステップS5)。

一方、暗証番号情報が一致している場合には、個人認証情報が入力手段21で選択される(ステップS6)。この場合、まず指紋情報が選択されると、カード使用者により指紋照合手段22から指紋情報データがホストコンピュータ24に入力される(ステップS7)。すると、ホストコンピュータ24から読み出手段23を通して、ICカード1の指紋情報エリアにアドレスポインタが移動される(ステップS8)。次に、指紋情報エリアに記憶されているアドレスにアドレスポインタが移動され(ステップS9)、アドレスポインタの示すアドレスから指紋情報データが読み出される(ステップS10)。そして、指紋照合手段22から入力された指紋情報データとICカード1から読み出された指紋情報データとが照合される(ス

テップS11)。その結果、指紋情報データが一致していない場合には、そのICカード1の正当な使用者ではないことから、ICカード1が読み出手段23から排出される。(ステップS12)。また、指紋情報データが一致している場合には、全ての情報の読み出しが終了したか否かが判定され(ステップS13)、その結果この時点ではまだ暗証番号情報および指紋情報の読み出しが終了していないことから、再びステップS6に戻って個人認証情報が入力手段21により選択される。

次に、画像情報が選択されると、ホストコンピュータ24から読み出手段23を通して、ICカード1の画像情報エリアにアドレスポインタが移動される(ステップS14)。次に、画像情報エリアに記憶されているアドレスにアドレスポインタが移動され(ステップS15)、アドレスポインタの示すアドレスから画像情報データが読み出される(ステップS16)。そして、この読み出した画像情報データが、編集して表示手段25に表示される(ステップS17)。次に、全ての情報の読み出しが終了したか否かが判定され(ステップS13)、その結果この時点では全ての情報の読み出しが終了していることから、ステップS12を移行してICカード1が読み出手段23から排出される。以上のようにして、ICカード

の読み出しが終了したか否かが判定され(ステップS13)、その結果この時点ではまだサイン情報の読み出しが終了していないことから、再びステップS6に戻って個人認証情報が入力手段21により選択される。

次に、サイン情報が選択されると、ホストコンピュータ24から読み出手段23を通して、ICカード1のサイン情報エリアにアドレスポインタが移動される(ステップS18)。次に、サイン情報エリアに記憶されているアドレスにアドレスポインタが移動され(ステップS19)、アドレスポインタの示すアドレスからサイン情報データが読み出される(ステップS20)。そして、この読み出したサイン情報データが、編集して表示手段25に表示される(ステップS17)。そして、全ての情報の読み出しが終了したか否かが判定され(ステップS13)、その結果この時点では全ての情報の読み出しが終了していることから、ステップS12を移行してICカード1が読み出手段23から排出される。以上のようにして、ICカード

1に対する特定情報の読み出しが行なわれる。

上述したように、本実施例の個人認証システムは、マイクロコンピュータ11、メモリ12を含むIC回路を搭載してなり、個人認証を必要とする業務における使用者を特定できる情報である、使用者の暗証番号情報、写真的画像情報、指紋情報、サイン情報を電気信号として記憶された個人認証用のICカード1と、暗証番号情報を入力する入力手段21、指紋情報を入力する指紋照合手段22、ICカード1に記憶された暗証番号情報、指紋情報、写真的画像情報およびサイン情報を読み出す読み出手段23、情報の読み出し処理を制御する機能、読み出した暗証番号情報ならびに指紋情報と入力情報との照合処理を行なう機能、読み出した写真的画像情報とサイン情報ならびに照合結果の表示処理を制御する機能を有するホストコンピュータ24、ホストコンピュータ24による処理内容を表示する表示手段25からなり、ICカード1に対して特定情報の読み出しを行なう個人認証情報読み出手段2とを備えて構成したものである。

従って、使用者の暗証番号情報、写真的画像情報、指紋情報、サイン情報等、その業務における使用者を特定できる情報を記憶容量の大きいICカード1に予め書き込んでおき、このICカード1の使用時に、当該ICカード1に記憶されている情報を読み出して入力情報との照合を行ない、特定の使用者を認証できるため、正当な使用者以外の者によってカードが不正に使用されるのを確実に防止することが可能となり、極めて信頼性の高い個人認証を行なうことができる。

尚、上記実施例では、使用者を特定できる情報として、使用者の暗証番号情報、写真的画像情報、指紋情報、サイン情報の全ての情報ICカード1に予め書き込んでおく場合について述べたが、本発明の所期の目的を達成するためには、使用者の暗証番号情報、写真的画像情報、指紋情報、サイン情報のうち、少なくとも写真的画像情報を予め書き込んでおけば十分である。

#### (発明の効果)

以上説明したように本発明によれば、使用者

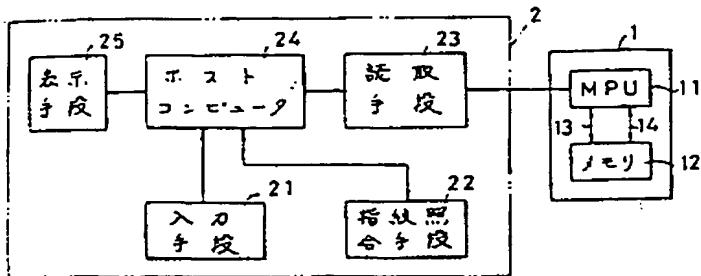
の暗証番号情報、写真的画像情報、指紋情報、サイン情報等、その業務における使用者を特定できる情報をICカードに予め書き込んでおき、このICカードの使用時に、当該ICカードに記憶されている情報を読み出して入力情報との照合を行ない、特定の使用者を認証できるようにしたので、個人認証を必要とする業務における正当な使用者の使用事実を特定して不正行為を確実に防止することが可能なICカードを用いた個人認証システムが提供できる。

#### 4. 図面の簡単な説明

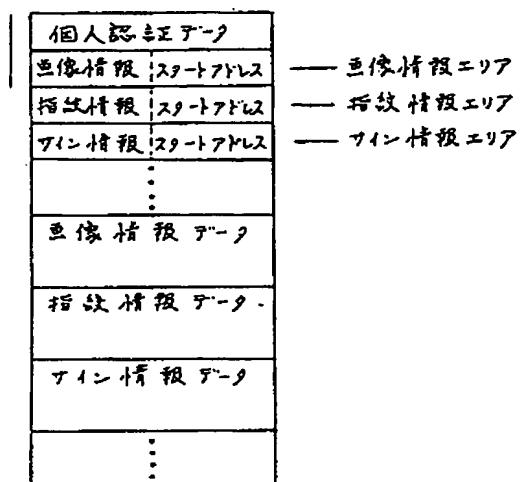
第1図は本発明によるICカードを用いた個人認証システムの一実施例を示すブロック図、第2図および第3図は同実施例における動作を説明するための図である。

1…ICカード、2…個人認証情報読み出手段、11…マイクロコンピュータ(MPU)、12…メモリ12、13…アドレスバス、14…データバス、21…入力手段、22…指紋照合手段、23…読み出手段、24…ホストコンピュータ、

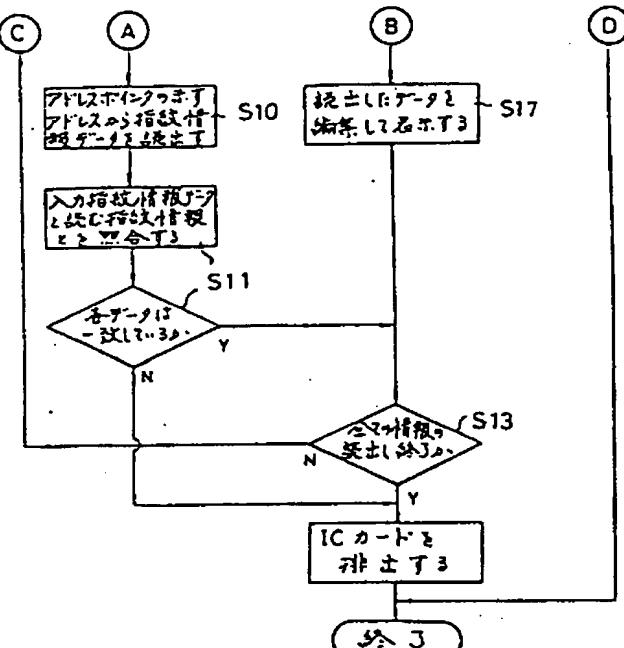
出願人代理人弁理士 細江武彦



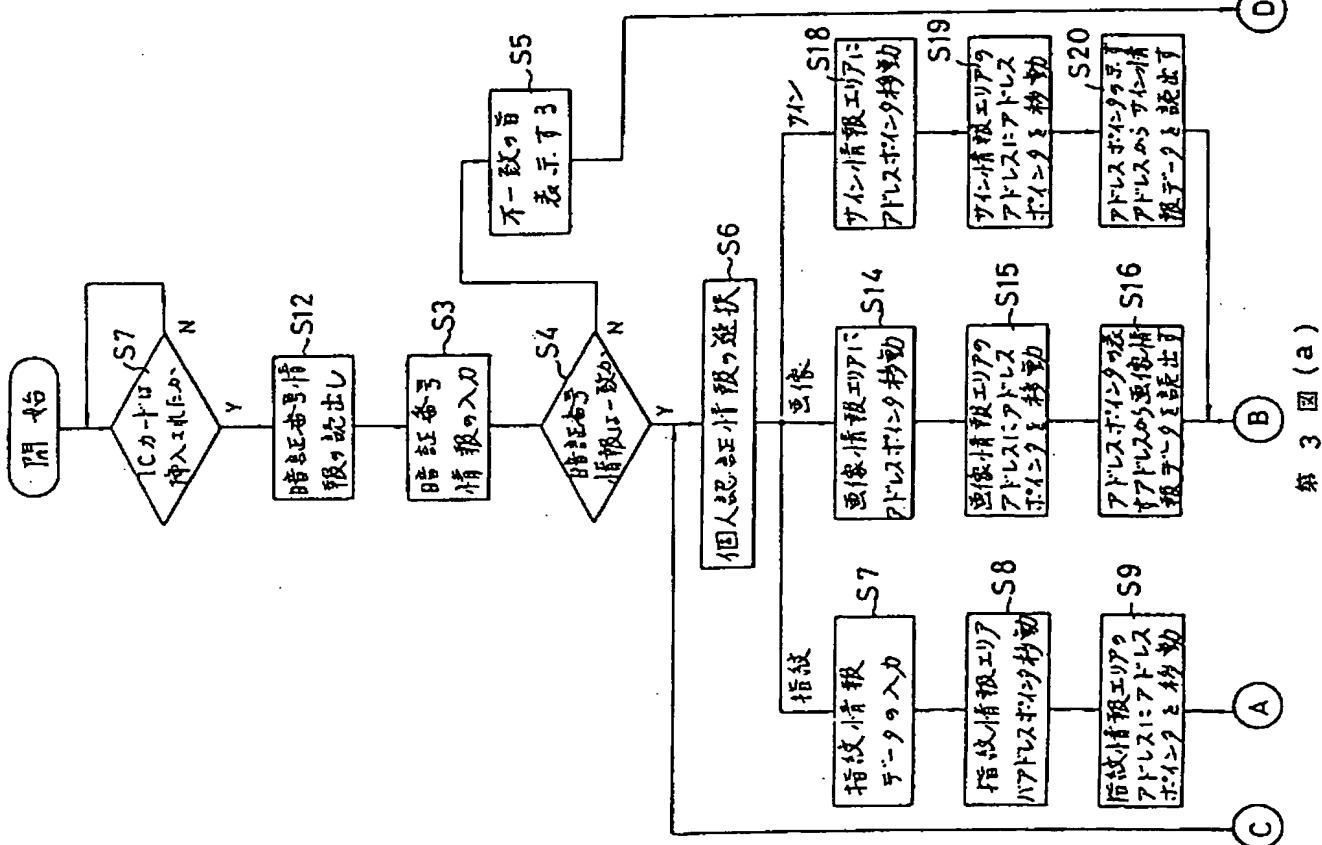
第 1 回



ప 2 త



### 第3圖(b)



第3図(a)